Isometry and Automorphisms of Constant Dimension Codes

Anna-Lena Trautmann
Institute of Mathematics
University of Zurich

Abstract

We define linear and semilinear isometry for general subspace codes, used for random network coding. Furthermore, some results on isometry classes and automorphism groups of known constant dimension code constructions are derived.

1 Introduction

Subspace codes are used for random linear network coding [1, 12]. They are defined as subsets of the projective geometry, which is the set of all subspaces of a given ambient space over a finite field. In the special case that all codewords have the same dimension, we call those codes *constant dimension codes*. It makes sense to define isometry classes of these codes and a canonical representative of each class to compare codes among each other.

On the other hand, a canonical form and the automorphism group are important for the theory of orbit codes [19], which are a special family of constant dimension codes. These codes are defined as orbits of a subgroup of the general linear group on an element of the projective geometry over a finite field. Different subgroups can possibly generate the same orbit, hence one needs a canonical way to compare orbit codes among each other. This can be done via the automorphism groups of the codes, since these are the maximal generating groups for a given orbit code and they contain all other generating subgroups of it.

The paper is structured as follows: We give some preliminary results in Section 2, first on network coding in general and on orbit codes. The second part of the section deals with linear and semilinear isometry of general subspace codes. It is shown that any (semi-)linearly isometric code of a given code can be reached by action of the projective (semi-)linear group.

In Section 3 we derive some theoretical results on and give some examples of isometry classes and automorphism groups of spread codes, orbit codes and lifted rank metric codes, which are known code constructions that will be explained in detail in that part.

We conclude in Section 4 by summing up the results.

2 Preliminaries

2.1 Network Coding

Let $\mathbb{F}_q$ be the finite field with q elements and the projective geometry $\mathrm{PG}(q,n)$ the set of all subspaces of $\mathbb{F}_q^n$, whereas $\mathcal{G}_q(k,n)$ is the set of all subspaces of $\mathbb{F}_q^n$ of dimension k, called *Grassmannian.* The general linear group $\mathrm{GL}_n(q)$ is the set of all invertible $n \times n$-matrices with entries in $\mathbb{F}_q$.

$\mathrm{Aut}(\mathbb{F}_q)$ denotes the automorphism group of $\mathbb{F}_q$. Recall that any automorphism α of a finite field of characteristic p is of the type $\alpha(x) = x^{p^j}$. It applies to vectors and matrices element-wise. Denote by $Gal(\mathbb{F}_{q^k}, \mathbb{F}_q)$ the Galois group of $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$, i.e. the set of all automorphisms of $\mathbb{F}_{q^k}$ that stabilize the subfield $\mathbb{F}_q$. If p is the characteristic of $\mathbb{F}_q$, then it holds that $\mathrm{Aut}(\mathbb{F}_q) = Gal(\mathbb{F}_q, \mathbb{F}_p)$.

The set of all semilinear mappings, i.e. the general semilinear group $\Gamma\mathrm{L}_n(q) := \mathrm{GL}_n(q) \rtimes \mathrm{Aut}(\mathbb{F}_q)$ decomposes as a semidirect product with the multiplication

$$(A, \alpha)(B, \beta) := (A\, \alpha^{-1}(B), \alpha\beta).$$

By $\mathrm{Mat}_{k\times n}(q)$ we denote the set of all $k \times n$-matrices with entries in $\mathbb{F}_q$. If the underlying field is clear from the context we abbreviate the above by $\mathrm{GL}_n, \Gamma\mathrm{L}_n$ and $\mathrm{Mat}_{k\times n}$, respectively.

Let $U \in \mathrm{Mat}_{k\times n}$ be a matrix of rank k and

$$\mathcal{U} = \mathrm{rs}(U) := \text{row space}(U) \in \mathcal{G}_q(k,n).$$

One notices that the row space is invariant under GL_k-multiplication on the left, i.e. for any $T \in \mathrm{GL}_k$

$$\mathcal{U} = \mathrm{rs}(U) = \mathrm{rs}(TU).$$

A unique representative of all matrices with the same row space is the one in reduced row echelon form. Any $k \times n$-matrix can be transformed into reduced row echelon form by a unique $T \in \mathrm{GL}_k$.

The *subspace distance* and the *injection distance* are metrics on the projective geometry $\mathrm{PG}(q,n)$ given by

$$\begin{aligned} d_S(\mathcal{U},\mathcal{V}) &= \dim(\mathcal{U}+\mathcal{V}) - \dim(\mathcal{U}\cap\mathcal{V}) \\ &= \dim(\mathcal{U}) + \dim(\mathcal{V}) - 2\dim(\mathcal{U}\cap\mathcal{V}) \end{aligned}$$

$$d_I(\mathcal{U},\mathcal{V}) = \max\{\dim(\mathcal{U}), \dim(\mathcal{V})\} - \dim(\mathcal{U}\cap\mathcal{V})$$

for any $\mathcal{U}, \mathcal{V} \in \mathrm{PG}(q,n)$. They are suitable distances for coding over the operator channel [12], where the injection metric is the more suitable one for an adversary model [15]. Since for $\mathcal{U}, \mathcal{V} \in \mathcal{G}_q(k,n)$ it holds that

$$d_S(\mathcal{U},\mathcal{V}) = 2d_I(\mathcal{U},\mathcal{V}),$$

they are exchangeable in the study of constant dimension codes. If we do not need to specify which metric we are using we will write $d(\mathcal{U},\mathcal{V})$.

In general a *subspace code* is simply a subset of $\mathrm{PG}(q,n)$. A *constant dimension code* is a subset of $\mathcal{G}_q(k,n)$. The minimum distance of a code is defined in the usual way.

Bounds on the size of subspace codes can be found in [6, 10, 12]. Different constructions of constant dimension codes have been investigated in e.g. [5, 11, 12, 16, 17, 19].

Given $U \in \mathrm{Mat}_{k\times n}$ of rank k, $\mathcal{U} \in \mathcal{G}_q(k,n)$ its row space and $(A,\alpha) \in \Gamma\mathrm{L}_n$, we define

$$\mathcal{U}(A,\alpha) := \mathrm{rs}(\alpha(UA)).$$

Since $\alpha(TUA) = \alpha(T)\alpha(UA)$ for any $T \in \mathrm{GL}_k$, the operation here defined is independent from the representation of $\mathcal{U}$ and therefore well-defined. The $\Gamma\mathrm{L}_n$-multiplication defines a group action from the right on the Grassmannian and hence on $\mathrm{PG}(q,n)$ as well:

$$\begin{array}{ccc} \mathcal{G}_q(k,n) \times \Gamma\mathrm{L}_n & \longrightarrow & \mathcal{G}_q(k,n) \\ (\mathcal{U},(A,\alpha)) & \longmapsto & \mathcal{U}(A,\alpha) \end{array}$$

This is indeed a group action since

$$(\mathcal{U}(A,\alpha))(B,\beta) = (\alpha(\mathcal{U}A))(B,\beta) = \beta(\alpha(\mathcal{U}A)B) = \beta\alpha((\mathcal{U}A)\alpha^{-1}(B))$$

$$= \alpha\beta(\mathcal{U}(A\alpha^{-1}(B))) = \mathcal{U}(A\alpha^{-1}(B),\alpha\beta) = \mathcal{U}((A,\alpha)(B,\beta)).$$

It induces a group action of GL_n on $\mathrm{PG}(q,n)$, too.

This action respects the distances d_S, d_I and therefore defines a notion of equivalence for subspace codes. In Section 2.2 we will show, that this equivalence is the most general one may demand if one also wants to preserve some other elementary properties of random subspace codes.

Generally, group actions on sets are performed element-wise. For a group G acting from the right on a set X and an element $x \in X$, $\mathrm{Stab}_G(x) := \{g \in G \mid xg = x\}$ denotes the stabilizer of x under G. The orbit of G on $x \in X$ is denoted by $xG := \{xg \mid g \in G\}$ and the set of all orbits by $X/\!\!/G := \{xG \mid x \in X\}$. A transversal of $X/\!\!/G$ is a set containing one element of each orbit.

An orbit $\mathcal{U}G, G \leq \mathrm{GL}_n$ on a point $\mathcal{U}$ of the Grassmannian is also called an *orbit code* [19]. Since

$$\mathcal{G}_q(k,n) \cong \mathrm{GL}_n/\mathrm{Stab}_{\mathrm{GL}_n}(\mathcal{U})$$

it is possible that different groups generate the same orbit code.

For the whole paper we will use vectors in row form and, if not stated differently, $\Gamma\mathrm{L}_n$ and GL_n will be applied from the right.

2.2 Isometry of Subspace Codes

An open question is how to define equivalence of subspace codes. Naturally equivalent codes should have the same ambient space, cardinality, error-correction capability (i.e. minimum distance) and transmission rate (for a fixed ambient space this is given by the maximal dimension of the codewords). Moreover, the distance distribution and the dimension distribution should be the same. Clearly, these last two conditions imply the minimum distance and maximum dimension.

This work engages in the isomorphic (with respect to the subset relation) equivalences of subspace codes.

Definition 1. A distance-preserving map $\iota : \mathrm{PG}(q,n) \to \mathrm{PG}(q,n)$ i.e. fulfilling

$$d(\mathcal{U},\mathcal{V}) = d(\iota(\mathcal{U}),\iota(\mathcal{V})) \quad \forall\, \mathcal{U},\mathcal{V} \in \mathrm{PG}(q,n).$$

is called an *isometry* on $\mathrm{PG}(q,n)$.

Any isometry ι is injective:

$$\mathcal{U} \neq \mathcal{V} \iff d(\mathcal{U},\mathcal{V}) \neq 0 \iff d(\iota(\mathcal{U}),\iota(\mathcal{V})) \neq 0 \iff \iota(\mathcal{U}) \neq \iota(\mathcal{V})$$

and hence, if the domain is equal to the co-domain, bijective. The inverse map ι^{-1} is an isometry as well.

Lemma 2. *If $\iota : \mathrm{PG}(q,n) \to \mathrm{PG}(q,n)$ is an isometry, then $\iota(\{0\}) \in \big\{\{0\},\mathbb{F}_q^n\big\}$.*

Proof. We will prove it using the subspace distance. The proof for the injection metric is analogous.

Assume $\mathcal{U} := \iota(\{0\}) \notin \big\{\{0\},\mathbb{F}_q^n\big\}$ and let $\mathcal{V} := \iota(\mathbb{F}_q^n)$. It holds that

$$\begin{aligned} & d_S(\{0\},\mathbb{F}_q^n) = d_S(\iota(\{0\}),\iota(\mathbb{F}_q^n)) \\ \iff \quad & n = d_S(\mathcal{U},\mathcal{V}) \\ \iff \quad & n = \dim(\mathcal{U}+\mathcal{V}) - \dim(\mathcal{U}\cap\mathcal{V}). \end{aligned}$$

This implies $\mathcal{U}+\mathcal{V} = \mathbb{F}_q^n$ and $\mathcal{U}\cap\mathcal{V} = \{0\}$ and thus $\mathcal{V} \notin \big\{\{0\},\mathbb{F}_q^n\big\}$. Choose non-zero vectors $u \in \mathcal{U}, v \in \mathcal{V}$ and consider the one-dimensional subspace $\mathcal{W}$ generated by $u+v$. Then $\dim(\mathcal{U}\cap\mathcal{W}) = \dim(\mathcal{V}\cap\mathcal{W}) = 0$ and

$$\begin{aligned} d_S(\iota^{-1}(\mathcal{W}),\{0\}) &= d_S(\mathcal{W},\mathcal{U}) = 1+\dim(\mathcal{U}) \\ d_S(\iota^{-1}(\mathcal{W}),\mathbb{F}_q^n) &= d_S(\mathcal{W},\mathcal{V}) = 1+\dim(\mathcal{V}) \end{aligned}$$

which leads to the following contradiction (recall that $d_S(\mathcal{X}, \{0\}) = \dim(\mathcal{X})$ and $d_S(\mathcal{X}, \mathbb{F}_q^n) = n - \dim(\mathcal{X})$ for any $\mathcal{X} \in \mathrm{PG}(q,n)$):

$$n = d_S(\iota^{-1}(\mathcal{W}), \{0\}) + d_S(\iota^{-1}(\mathcal{W}), \mathbb{F}_q^n) = 2 + \dim(\mathcal{U}) + \dim(\mathcal{V}) = 2 + n$$

□

Lemma 3. *Let ι be as before and $\mathcal{U} \in \mathrm{PG}(q,n)$ arbitrary. Then*

$$\iota(\{0\}) = \{0\} \Longrightarrow \dim(\mathcal{U}) = d(\{0\}, \mathcal{U}) = d(\{0\}, \iota(\mathcal{U})) = \dim(\iota(\mathcal{U}))$$

and on the other hand

$$\iota(\{0\}) = \mathbb{F}_q^n \Longrightarrow \dim(\mathcal{U}) = d(\{0\}, \mathcal{U}) = d(\mathbb{F}_q^n, \iota(\mathcal{U})) = n - \dim(\iota(\mathcal{U})).$$

In the following, we restrict ourselves to the isometries with $\iota(\{0\}) = \{0\}$ because these are exactly the isometries that keep the dimension of a codeword. Now we want to characterize all isometries on $\mathrm{PG}(q,n)$ with $\iota(\{0\}) = \{0\}$. For it we need the Fundamental Theorem of Projective Geometry (cf. [2, 3]):

Theorem 4. *Let $\mathcal{Z}_n := \{\mu I_n \mid \mu \in \mathbb{F}_q^*\}$ be the set of scalar transformations. Then every order-preserving bijection (with respect to the subset relation) $f : \mathrm{PG}(q,n) \to \mathrm{PG}(q,n)$, where $n > 2$, is induced by a semilinear transformation $(A, \alpha) \in$*

$$\mathrm{P\Gamma L}_n = (\mathrm{GL}_n / \mathcal{Z}_n) \rtimes \mathrm{Aut}(\mathbb{F}_q).$$

Theorem 5. *For $n > 2$ a map $\iota : \mathrm{PG}(q,n) \to \mathrm{PG}(q,n)$ is an order-preserving bijection (with respect to the subset relation) of $\mathrm{PG}(q,n)$ if and only if it is an isometry with $\iota(\{0\}) = \{0\}$.*

Proof. We will again prove the statement using the subspace distance, where an analogous proof holds for the injection distance.

1. "$\Longleftarrow$"

   Let ι be an isometry with $\iota(\{0\}) = \{0\}$. We have to show that for any $\mathcal{U}, \mathcal{V} \in \mathrm{PG}(q,n)$ the following holds:

   $$\mathcal{U} \subseteq \mathcal{V} \Longleftrightarrow \iota(\mathcal{U}) \subseteq \iota(\mathcal{V})$$

   From Lemma 3 one knows that $\dim(\mathcal{U}) = \dim(\iota(\mathcal{U}))$. Assume that there are $\mathcal{U}, \mathcal{V} \in \mathrm{PG}(q,n)$ with $\mathcal{U} \subseteq \mathcal{V}$ and $\iota(\mathcal{U}) \not\subseteq \iota(\mathcal{V})$. This leads to the contradiction:

   $$\begin{aligned} d_S(\iota(\mathcal{U}), \iota(\mathcal{V})) &= \dim(\iota(\mathcal{U})) + \dim(\iota(\mathcal{V})) - 2\dim(\iota(\mathcal{U}) \cap \iota(\mathcal{V})) \\ &> \dim(\iota(\mathcal{U})) + \dim(\iota(\mathcal{V})) - 2\dim(\iota(\mathcal{U})) \\ &= \dim(\mathcal{U}) + \dim(\mathcal{V}) - 2\dim(\mathcal{U}) \\ &= \dim(\mathcal{U}) + \dim(\mathcal{V}) - 2\dim(\mathcal{U} \cap \mathcal{V}) \\ &= d_S(\mathcal{U}, \mathcal{V}) \end{aligned}$$

Hence $\mathcal{U} \subseteq \mathcal{V} \implies \iota(\mathcal{U}) \subseteq \iota(\mathcal{V})$. Since ι^{-1} is an isometry as well, the converse also holds. Thus, ι is an order-preserving bijection.

2. "$\Longrightarrow$"
   According to Theorem 4 any order-preserving bijection ι of the projective geometry can be expressed by a pair $(A, \alpha) \in \mathrm{P\Gamma L}_n$. Then

$$\begin{aligned} d_S(\iota(\mathcal{U}), \iota(\mathcal{V})) &= d_S(\alpha(\mathcal{U}A), \alpha(\mathcal{V}A)) \\ &= \dim(\alpha(\mathcal{U}A)) + \dim(\alpha(\mathcal{V}A)) - 2\dim(\alpha(\mathcal{U}A) \cap \alpha(\mathcal{V}A)) \\ &= \dim(\mathcal{U}) + \dim(\mathcal{V}) - 2\dim(\alpha((\mathcal{U} \cap \mathcal{V})A)) \\ &= d_S(\mathcal{U}, \mathcal{V}) \end{aligned}$$

   thus ι is an isometry with $\iota(\{0\}) = \{0\}$.

□

Corollary 6. *Every isometry ι on $\mathrm{PG}(q, n)$, where $n > 2$, with $\dim(\mathcal{U}) = \dim(\iota(\mathcal{U}))$ for any $\mathcal{U} \in \mathrm{PG}(q, n)$ is induced by a semilinear transformation $(A, \alpha) \in \mathrm{P\Gamma L}_n$.*

From now on assume that $n > 2$. This is no real restriction, because for application, subspace codes in an ambient space of dimension 2 are not interesting since the only non-trivial subspaces are the one-dimensional ones. In that case neither the transmission rate is improved compared to forwarding, nor is error-correction possible.

Definition 7. 1. Two codes $\mathcal{C}_1, \mathcal{C}_2 \subseteq \mathrm{PG}(q, n)$ are *linearly isometric* if there exists $A \in \mathrm{PGL}_n$ such that $\mathcal{C}_1 = \mathcal{C}_2 A$. Since it is the orbit of PGL_n on the code, the set of all linearly isometric codes is denoted by $\mathcal{C}_1\mathrm{PGL}_n$.

2. We call $\mathcal{C}_1$ and $\mathcal{C}_2$ *semilinearly isometric* if there exists $(A, \alpha) \in \mathrm{P\Gamma L}_n$ such that $\mathcal{C}_1 = \mathcal{C}_2(A, \alpha)$. The set of all semilinearly isometric codes is denoted by $\mathcal{C}_1\mathrm{P\Gamma L}_n$.

Clearly linear and semilinear isometry are equivalence relations, so it makes sense to speak of classes of (semi-)linearly isometric codes. Note, that the isometries are independent of the underlying metric.

A lattice point-of-view of the isometries of subspace codes can be found in [18].

Definition 8. The set

$$\mathrm{SAut}(\mathcal{C}) := \mathrm{Stab}_{\Gamma\mathrm{L}_n}(\mathcal{C}) := \{(A, \alpha) \in \Gamma\mathrm{L}_n \mid \mathcal{C}(A, \alpha) = \mathcal{C}\}$$

is a subgroup of $\Gamma\mathrm{L}_n$ and is called the *semi-linear automorphism group* of the subspace code $\mathcal{C}$. The *(linear) automorphism group* of $\mathcal{C}$ is defined as

$$\mathrm{Aut}(\mathcal{C}) := \mathrm{Stab}_{\mathrm{GL}_n}(\mathcal{C}) := \{A \in \mathrm{GL}_n \mid \mathcal{C}A = \mathcal{C}\}$$

and is a subgroup of $\mathrm{SAut}(\mathcal{C})$.

Note, that $\mathrm{Aut}(\mathcal{U}G)$ contains every subgroup of GL_n that generates the orbit $\mathcal{U}G$.

Lemma 9. *For a subspace code $\mathcal{C} := \{\mathrm{rs}(U_i) \mid i = 1, \dots, m\} \subseteq \mathcal{G}_q(k, n)$ we know that*

$$\bigcap_{i=1}^{m} \mathrm{Stab}_{\mathrm{GL}_n}(\mathrm{rs}(U_i)) \subseteq \mathrm{Aut}(\mathcal{C}).$$

Since

$$B \in \bigcap_{i=1}^{l} \mathrm{Stab}_{\mathrm{GL}_n}(\mathrm{rs}(U_i)) \iff \exists A \in \mathrm{GL}_k : AU_i = U_i B \ \ \forall i = 1, \dots, l$$

we conclude that in particular $\lambda I_n \in \mathrm{Aut}(\mathcal{C})$ for all $\lambda \in \mathbb{F}_q \setminus \{0\} =: \mathbb{F}_q^*$.

Therefore, one can replace the projective groups with GL_n and $\Gamma\mathrm{L}_n$ when computing isometry classes and automorphism groups of subspace codes.

3 Isometry and Automorphisms of Known Code Constructions

In this section we will examine the isometries and automorphism groups of some known classes of constant dimension codes, namely spread codes, orbit codes and lifted rank metric codes.

3.1 Spread codes

Spreads of vector spaces are well-known geometrical objects, defined to be partitions of the non-zero elements of a given vector space into subspaces (without the zero-element) of that vector space of a fixed dimension. I.e. a k-spread of $\mathbb{F}_q^n$ is a set of subspaces of dimension k such that they pairwise intersect only trivially and they cover the whole vector space $\mathbb{F}_q^n$. Thus, a spread exists if and only if $k|n$ and is a subset of $\mathcal{G}_q(k, n)$, i.e. it can be used as a constant dimension code. In this case we speak of a *spread code*. A spread code has cardinality $(q^n - 1)/(q^k - 1)$ and minimum distance $2k$.

Different constructions for these codes are known and have been studied from a coding perspective, e.g. in [8, 13, 14].

The trivial cases are $k = 1$ where the spread corresponds to the projective space and $k = n$ where the spread has one element, namely the whole space.

One way of constructing spreads is the $\mathbb{F}_{q^k}$-linear representation of $\mathbb{F}_{q^n}$: Since $k|n$ we can consider $\mathbb{F}_{q^n}$ as an extension field of $\mathbb{F}_{q^k}$ of degree $l := n/k$, which is isomorphic to the vector space $\mathbb{F}_{q^k}^l$. In this vector space consider the trivial spread of all one-dimensional subspaces. Each of these lines over $\mathbb{F}_{q^k}$ can now be considered as a k-dimensional subspace over $\mathbb{F}_q$. Since the lines of $\mathbb{F}^l_{q^k}$ intersect only trivially and with a simple counting argument it follows that the corresponding k-dimensional subspaces of $\mathbb{F}_q^n$ form a spread.

We call a spread code *Desarguesian* if it is an $\mathbb{F}_{q^k}$-linear representation of $\mathbb{F}_{q^n}$, or if it is a column permutation of such a code.

Theorem 10. *All Desarguesian spread codes are linearly isometric.*

Proof. Since there is only one spread of lines in $\mathbb{F}^l_{q^k}$, different Desarguesian spreads of $\mathbb{F}_q^n$ can only arise from the different isomorphisms between $\mathbb{F}_{q^k}$ and $\mathbb{F}_q^k$. As the isomorphisms are linear maps, there exists a linear map between the different spreads arising from them. □

In general, not all spreads are linearly isometric but in the special case of $q = 2, k = 2, n = 4$ they actually are, which can be seen as follows. From [9, Lemma 17.1.3] we know that every spread in $\mathcal{G}_q(2,4)$ is regular. Since in $\mathcal{G}_2(k,2k)$ a spread is Desarguesian if and only if it is regular [9, p. 207], we know that every spread is Desarguesian. Hence all spreads in $\mathcal{G}_q(2,4)$ are linearly isometric.

We will now investigate the automorphism groups of Desarguesian spreads.

Theorem 11. *The linear automorphism group of a Desarguesian spread code $\mathcal{C} \subseteq \mathcal{G}_q(k,n)$ is isomorphic to $\mathrm{GL}_{\frac{n}{k}}(q^k) \times Gal(\mathbb{F}_{q^k}, \mathbb{F}_q)$.*

Proof. Let $l := n/k$. We want to find all $\mathbb{F}_q$-linear bijections of $\mathbb{P}^{l-1}(\mathbb{F}_{q^k})$. We know that $\mathrm{PGL}_l(q^k)$ is the groups of all $\mathbb{F}_{q^k}$-linear bijections of $\mathbb{P}^{l-1}(\mathbb{F}_{q^k})$. Thus, $\mathrm{PGL}_l(q^k) \times Gal(\mathbb{F}_{q^k}, \mathbb{F}_q)$ is the set of all $\mathbb{F}_q$-linear bijections of $\mathbb{P}^{l-1}(\mathbb{F}_{q^k})$. It follows that in the affine space the linear automorphism group of such a spread is isomorphic to $\mathrm{GL}_l(q^k) \times Gal(\mathbb{F}_{q^k}, \mathbb{F}_q)$. □

Corollary 12. *Let $\mathcal{S}$ be a Desarguesian spread code in $\mathcal{G}_q(k,n)$. Then*

$$|\mathrm{Aut}(\mathcal{S})| = k \prod_{i=0}^{\frac{n}{k}-1} q^n - q^{ki}.$$

Proof. Follows from the fact that $|Gal(\mathbb{F}_{q^k}, \mathbb{F}_q)| = k$ and $|\mathrm{GL}_{\frac{n}{k}}(q^k)| = \prod_{i=0}^{n/k-1} (q^k)^{\frac{n}{k}} - (q^k)^i$. □

Since $\mathbb{F}_{q^k}$ is isomorphic to $\mathbb{F}_q[\alpha]$ where α is a root of an irreducible polynomial $p(x)$ of degree k but also to $\mathbb{F}_q[P]$ where P the companion matrix of $p(x)$, we get:

Corollary 13. *The automorphism group of a Desarguesian spread code in $\mathcal{G}_q(k,n)$ is generated by all elements in GL_n where the $k \times k$-blocks are elements of $\mathbb{F}_q[P]$ and block diagonal matrices where the blocks represent an automorphism of $\mathbb{F}_{q^k}$.*

Another point of view of the construction of a Desarguesian spread can be found in [13], where the generator matrices of the code words are of the type

$$U = \left[\begin{array}{cccc} B_1 & B_2 & \dots & B_l \end{array} \right]$$

where the blocks B_i are an element of $\mathbb{F}_q[P]$ and P is a companion matrix of an irreducible polynomial of degree k. To stay inside this structure (i.e. to apply an automorphism) we can permute the blocks, do block-wise multiplications or do block-wise additions with elements from $\mathbb{F}_q[P]$. This coincides with the structure of the automorphism groups from before.

This result is depicted in the following Examples.

Example 14. Consider $\mathcal{G}_2(2,4)$. The only binary irreducible polynomial of degree 2 is $p(x) = x^2 + x + 1$, i.e.

$$P = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

The respective spread code is

$$\mathcal{C} = \{\mathrm{rs}\left[\begin{array}{cc} I & 0 \end{array} \right], \mathrm{rs}\left[\begin{array}{cc} I & I \end{array} \right], \mathrm{rs}\left[\begin{array}{cc} I & P \end{array} \right], \mathrm{rs}\left[\begin{array}{cc} I & P^2 \end{array} \right], \mathrm{rs}\left[\begin{array}{cc} 0 & I \end{array} \right]\}$$

and its automorphism group has 360 elements:

$$\mathrm{Aut}(\mathcal{C}) = \left\langle \begin{pmatrix} & I \\ I & \end{pmatrix}, \begin{pmatrix} I & \\ & P \end{pmatrix}, \begin{pmatrix} I & P \\ & I \end{pmatrix}, \begin{pmatrix} Q & \\ & Q \end{pmatrix} \right\rangle$$

where $Q = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \in \mathrm{GL}_2$ represents the only non-trivial automorphism of $\mathbb{F}_{2^2}$, i.e. $x \mapsto x^2$.

A different approach of finding the automorphism group of a spread in $\mathcal{G}_2(2,4)$ can also be found in [9, Corollary 2].

Example 15. Consider $\mathcal{G}_3(2,4)$ and the irreducible polynomial $p(x) = x^2 + x + 2$, i.e.

$$P = \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}$$

The spread code is

$$\mathcal{C} = \mathrm{rs}\left[\begin{array}{cc} I & 0 \end{array} \right] \cup \{\mathrm{rs}\left[\begin{array}{cc} I & P^i \end{array} \right] \mid i = 0, \dots, 7\} \cup \mathrm{rs}\left[\begin{array}{cc} 0 & I \end{array} \right]$$

and its automorphism group has 11520 elements:

$$\mathrm{Aut}(\mathcal{C}) = \left\langle \begin{pmatrix} & I \\ I & \end{pmatrix}, \begin{pmatrix} I & \\ & P \end{pmatrix}, \begin{pmatrix} I & P \\ & I \end{pmatrix}, \begin{pmatrix} Q & \\ & Q \end{pmatrix} \right\rangle$$

where $Q = \begin{pmatrix} 1 & 0 \\ 2 & 2 \end{pmatrix} \in \mathrm{GL}_2$. Here Q represents the only non-trivial automorphism of $\mathbb{F}_{3^2}$, i.e. $x \mapsto x^3$.

Note, that in both examples the first element of the generator sets corresponds to swapping the blocks, the second corresponds to multiplication by P and the third element to adding P in the second block of the code word generator matrices.

3.2 Orbit codes

Orbit codes are defined as orbits under the group action of the general linear group on the Grassmannian, which is defined as follows:

$$\begin{aligned} \mathcal{G}_q(k,n) \times \mathrm{GL}_n &\longrightarrow \mathcal{G}_q(k,n) \\ (\mathcal{U}, A) &\longmapsto \mathcal{U}A \end{aligned}$$

They were first defined in [19]. For more information on orbit codes the reader is referred to [18], where also a similar version of the following fact on isometry of orbit codes can be found:

Theorem 16. *Let $\mathcal{C}_1 = \mathcal{U}_1 G$ be an orbit code. Then $\mathcal{C}_2$ is linearly (respectively semilinearly) isometric to $\mathcal{C}_1$ if and only if there exists $S \in \mathrm{GL}_n$ (respectively $S \in \mathrm{PGL}_n$) such that*

$$\mathcal{C}_2 = \mathcal{U}_1 S(S^{-1}GS),$$

i.e. $S^{-1}GS$ is a defining group of $\mathcal{C}_2$.

For a given orbit code $\mathcal{C} \in \mathcal{G}_q(k,n)$ we call any subgroup $G \leq \mathrm{GL}_n$ a *generating group* of $\mathcal{C}$, if $\mathcal{U}G = \mathcal{C}$ for some $\mathcal{U} \in \mathcal{C}$.

If the generating groups of two orbit codes are cyclic, they are conjugate in GL_n if and only if the rational canonical forms of their generators have the same number of elementary divisors of the same degree and order and the same respective exponents of the elementary divisors [18, Section 4].

As mentioned in the beginning, the automorphism groups can be seen as a canonical representative of the generating groups of orbit codes.

Proposition 17.

- *Every generating group of an orbit code is a subgroup of the automorphism group.*
- *Every subgroup of the automorphism group containing a generating group is a generating group. Hence, the automorphism group is a generating group of the orbit code.*

Proof.

- If $\mathcal{C} = \mathcal{U}G$, then $\mathcal{C}G = \mathcal{U}GG = \mathcal{U}G$.
- Let G be a generating group of $\mathcal{C}$ and $G \leq H \leq \mathrm{Aut}(\mathcal{C})$. Hence, $\mathcal{C} = \mathcal{U}G$ and $\mathcal{C}H = \mathcal{C}$. This implies that $\mathcal{U}H = \mathcal{U}GH = \mathcal{C}H = \mathcal{C}$, since G is a subgroup of H.

□

The question of finding elements of the automorphism group can be translated into a stabilizer condition of the initial point of the orbit.

Proposition 18. *$A \in \mathrm{GL}_n$ is in the automorphism group of $\mathcal{C} = \mathcal{U}G$ if and only if for every $B' \in \mathrm{GL}_n$ there exists a $B'' \in \mathrm{GL}_n$ such that*

$$B'AB'' \in \mathrm{Stab}_{\mathrm{GL}_n}(\mathcal{U}).$$

Proof.

$$\begin{aligned} A \in \mathrm{Aut}(\mathcal{C}) &\iff \mathcal{C}A = \mathcal{C} \\ &\iff \forall B' \in G\, \exists B^* \in G :\ \mathcal{U}B'A = \mathcal{U}B^* \\ &\iff \forall B' \in G\, \exists B^* \in G :\ \mathcal{U}B'AB^{*-1} = \mathcal{U} \end{aligned}$$

The statement follows with $B'' := B^{*-1} \in G$. □

3.3 Lifted rank-metric codes

Rank-metric codes are matrix codes, i.e. subsets of $\mathrm{Mat}_{k\times m}$ (in this work we will restrict ourselves to the case $k \leq m$) equipped with the rank distance

$$d_R(U,V) := \mathrm{rank}(U-V) \quad \text{for } U,V \in \mathrm{Mat}_{k\times m}.$$

Naturally such a matrix code can also be seen as a block code in $\mathbb{F}_{q^k}^m$. We will denote rank-metric codes by $\mathcal{C}_R$.

The isometry of rank-metric codes has already been studied in [4]:

Lemma 19.

1. *The set of $\mathbb{F}_{q^k}$-linear isometries on $\mathbb{F}_{q^k}^m$ equipped with the rank-metric is $\mathcal{R}^{lin}(\mathbb{F}_{q^k}^m) := \mathrm{GL}_m(q) \times \mathbb{F}_{q^k}^*$.*
2. *The set of $\mathbb{F}_{q^k}$-semilinear isometries on $\mathbb{F}_{q^k}^m$ equipped with the rank-metric is $\mathcal{R}^{semi}(\mathbb{F}_{q^k}^m) := \left(\mathrm{GL}_m(q) \times \mathbb{F}_{q^k}^*\right) \rtimes \mathrm{Aut}(\mathbb{F}_{q^k})$.*

For the matrix representation of rank-metric codes we can replace $\mathbb{F}_{q^k}$ with $\mathbb{F}_q[P]$ where P is the companion matrix of an irreducible polynomial of degree k. The multiplication with elements from $\mathbb{F}_q[P]$ is done from the left.

Note, that an $\mathbb{F}_{q^k}$-linear map is also $\mathbb{F}_q$-linear. On the other hand, there might be other $\mathbb{F}_q$-(semi-)linear isometries than the ones mentioned before.

One can create constant dimension codes from a given rank-metric code, as explained in the following.

Lemma 20. *[16] Let $\mathcal{C}_R \subseteq \mathrm{Mat}_{k\times n-k}$ be a rank-metric code with minimum distance d. Then the lifted code*

$$\mathcal{C} = \{\mathrm{rs}\,[\,I_k \;\; A\,] \mid A \in \mathcal{C}_R\}$$

is a constant dimension code in $\mathcal{G}_q(k,n)$ with minimum distance $2d$.

Proposition 21. *The following elements map a lifted rank-metric code to another lifted rank-metric code with the same parameters and are semilinear isometries:*

$$\left\{ (\begin{pmatrix} I_k & \\ & A \end{pmatrix}, \alpha) \mid A \in \mathrm{GL}_{n-k}, \alpha \in \mathrm{Aut}(\mathbb{F}_q) \right\}$$

For $\alpha = id$ they are linear isometries.

Proof. Follows from the block matrix multiplication rules with

$$\begin{bmatrix} I_k & B \end{bmatrix} \begin{pmatrix} I_k & \\ & A \end{pmatrix} = \begin{bmatrix} I_k & BA \end{bmatrix}$$

and the fact that A is a rank-metric isometry. Moreover, $\alpha I_k = I_k$ and α is a rank-metric isometry since $\mathrm{Aut}(\mathbb{F}_{q^k}) \supseteq \mathrm{Aut}(\mathbb{F}_q)$. □

Corollary 22. *If two rank-metric codes are $\mathbb{F}_{q^k}$-linearly isometric in the rank-metric space, their lifted codes are linearly isometric in the Grassmannian.*

Proof. Let $\mathcal{C}_R$ and $\mathcal{C}'_R$ be two linearly isometric rank-metric codes, i.e. $\mathcal{C}'_R = P'\mathcal{C}_R A$ with $P' \in \mathbb{F}_q[P]$ and $A \in \mathrm{GL}_{n-k}$. Then the lifted code of $\mathcal{C}'_R$ is

$$\begin{aligned}
\mathcal{C}' &= \{\mathrm{rs} \begin{bmatrix} I_k & R' \end{bmatrix} \mid R' \in \mathcal{C}_{R'}\} \\
&= \{\mathrm{rs} \begin{bmatrix} I_k & P'RA \end{bmatrix} \mid R \in \mathcal{C}_R\} \\
&= \{\mathrm{rs} \begin{bmatrix} P'^{-1} & R \end{bmatrix} \mid R \in \mathcal{C}_R\} \begin{pmatrix} I_k & \\ & A \end{pmatrix} \\
&= \{\mathrm{rs} \begin{bmatrix} I_k & R \end{bmatrix} \mid R \in \mathcal{C}_R\} \begin{pmatrix} P'^{-1} & \\ & A \end{pmatrix} \\
&= \mathcal{C} \begin{pmatrix} P'^{-1} & \\ & A \end{pmatrix}
\end{aligned}$$

where $\mathcal{C}$ is the lifted code of $\mathcal{C}_R$. Hence, the lifted codes are linearly isometric. □

Naturally, there are codes that are linearly isometric to a lifted rank-metric code but are not a lifted rank-metric code itself.

We can use the knowledge of the automorphism group of a rank-metric code also for finding the automorphism group of the respective lifted rank-metric code. For this denote by Aut_R the automorphism group of the rank-metric code.

Proposition 23. *Let $\mathcal{C}_R \subseteq \mathrm{Mat}_{k\times(n-k)}$ be a rank-metric code and $\mathcal{C}$ its lifted code. Then*

$$\left\{ \begin{pmatrix} I_k & \\ & R \end{pmatrix} \mid R \in \mathrm{Aut}_R(\mathcal{C}_R) \right\} \subseteq \mathrm{Aut}(\mathcal{C}).$$

Proof. It holds that

$$\{[\begin{array}{cc} I_k & B \end{array}] \mid B \in \mathcal{C}_R\} \begin{pmatrix} I_k & \\ & R \end{pmatrix} = \{[\begin{array}{cc} I_k & BR \end{array}] \mid B \in \mathcal{C}_R\}.$$

Since $R \in \operatorname{Aut}_R(\mathcal{C}_R)$, this set is equal to the original one. □

Theorem 24. *Let $\mathcal{C}_R \subseteq \operatorname{Mat}_{k\times(n-k)}$ be a rank-metric code and $\mathcal{C}$ its lifted code. Then*

$$\left\{\begin{pmatrix} I_k & \\ & A \end{pmatrix} \mid A \in \operatorname{GL}_{n-k}\right\} \cap \operatorname{Aut}(\mathcal{C}) = \left\{\begin{pmatrix} I_k & \\ & R \end{pmatrix} \mid R \in \operatorname{Aut}_R(\mathcal{C}_R)\right\}.$$

Proof. From Proposition 23 we know that the right side is included in the left. Furthermore,

$$\operatorname{rs}[\begin{array}{cc} I_k & B_1 \end{array}] \begin{pmatrix} I_k & \\ & A \end{pmatrix} = \operatorname{rs}[\begin{array}{cc} I_k & B_2 \end{array}]$$

$$\iff \exists C_1, C_2 \in \operatorname{GL}_k : [\begin{array}{cc} C_1 & C_1 B_1 \end{array}] \begin{pmatrix} I_k & \\ & A \end{pmatrix} = [\begin{array}{cc} C_2 & C_2 B_2 \end{array}]$$

$$\iff C_1 = C_2 \quad \wedge \quad B_1 A = B_2$$

i.e. if $\begin{pmatrix} I_k & \\ & A \end{pmatrix} \in \operatorname{Aut}(\mathcal{C})$, then $A \in \operatorname{Aut}_R(\mathcal{C}_R)$. □

Hence, if we know the automorphism group of a lifted rank-metric code, we also know the automorphism group of the rank-metric code itself.

Example 25. Consider the rank-metric code

$$\mathcal{C}_R = \left\{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\right\}$$

with four elements and minimum rank distance 1 over $\mathbb{F}_2$. Its automorphism group is

$$\operatorname{Aut}_R(\mathcal{C}_R) = \left\{\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in \mathbb{F}_2\right\}.$$

Let $\mathcal{C}$ be the lifted code of $\mathcal{C}_R$ in $\mathcal{G}_2(2,4)$. Then

$$\operatorname{Aut}(\mathcal{C}) = \left\langle \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \right.$$

$$\left. \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \right\rangle$$

with $|\operatorname{Aut}(\mathcal{C})| = 192$. The second generator and the identity matrix are the corresponding elements described in Theorem 24.

4 Conclusion

In this work we investigated linear and semilinear isometry, as well as linear and semilinear automorphism groups, for general network codes, i.e. sets of vector spaces over a finite field. We showed that the subset-relation-and-dimension-preserving isometries correspond exactly to the general (semi-)linear group.

In Section 3 we showed some theoretical results and examples of isometry classes and automorphism groups of some known constructions of constant dimension codes, namely spread codes, orbit codes and lifted rank metric codes.

The isometry classes indicate how many non-equivalent different codes for given size and minimum distance can be found. On the other hand, the automorphism groups are useful for counting how many different codes there are in the same isometry class of a given code.

Moreover, the automorphism groups of orbit codes function as a canonical generating group to compare orbit codes among each other.

More research can be done in finding theoretical results on the automorphism groups of constant dimension codes. E.g. one could study the automorphism groups of non-Desarguesian spreads or try to find a family of orbit codes that have a certain automorphism group. Moreover, one could study the isometry and automorphism groups of non-constant dimension codes.

In general, it might not always be possible to compute the automorphism group of an arbitrary subspace code or check if two given codes are isometric. In this case, the algorithm of T. Feulner in [7] can be used to do these computations.

For future work it would be interesting to see how the knowledge of the automorphism group of a given constant dimension code (or a general subspace code) can be helpful for decoding, as it is in the classical block code case.

Acknowledgements

The author thanks Thomas Feulner, without whom this work would not have been possible, as well as Joachim Rosenthal and Leo Storme for their advice.

References

[1] R. Ahlswede, N. Cai, S.-Y.R. Li, and R.W. Yeung. Network information flow. *Information Theory, IEEE Transactions on*, 46(4):1204–1216, July 2000.

[2] E. Artin. *Geometric algebra*. Interscience tracts in pure and applied mathematics. John Wiley & Sons, 1988.

[3] R. Baer. *Linear algebra and projective geometry*. Pure and applied mathematics. Academic Press, 1952.

[4] T.P. Berger. Isometries for rank distance and permutation group of gabidulin codes. *Information Theory, IEEE Transactions on*, 49(11):3016 – 3019, nov. 2003.

[5] T. Etzion and N. Silberstein. Error-correcting codes in projective spaces via rank-metric codes and Ferrers diagrams. *IEEE Trans. Inform. Theory*, 55(7):2909–2919, 2009.

[6] T. Etzion and A. Vardy. Error-correcting codes in projective space. In *Information Theory, 2008. ISIT 2008. IEEE International Symposium on*, pages 871–875, July 2008.

[7] T. Feulner. Canonical forms and automorphisms in the projective space. *preprint*, 2012.

[8] E. Gorla, F. Manganiello, and J. Rosenthal. An algebraic approach for decoding spread codes. *arXiv:1107.55230v1*, [cs.IT], 2011.

[9] J. W. P. Hirschfeld. *Finite projective spaces of three dimensions*. Oxford Mathematical Monographs. The Clarendon Press Oxford University Press, New York, 1985. Oxford Science Publications.

[10] A. Khaleghi, D. Silva, and F. R. Kschischang. Subspace codes. In *IMA Int. Conf.*, pages 1–21, 2009.

[11] A. Kohnert and S. Kurz. Construction of large constant dimension codes with a prescribed minimum distance. In Jacques Calmet, Willi Geiselmann, and Jörn Müller-Quade, editors, *MMICS*, volume 5393 of *Lecture Notes in Computer Science*, pages 31–42. Springer, 2008.

[12] R. Kötter and F.R. Kschischang. Coding for errors and erasures in random network coding. *Information Theory, IEEE Transactions on*, 54(8):3579–3591, August 2008.

[13] F. Manganiello, E. Gorla, and J. Rosenthal. Spread codes and spread decoding in network coding. In *Proceedings of the 2008 IEEE International Symposium on Information Theory*, pages 851–855, Toronto, Canada, 2008.

[14] F. Manganiello and A.-L. Trautmann. Spread decoding in extension fields. *arXiv:1108.5881v1*, [cs.IT], 2011.

[15] D. Silva and F.R. Kschischang. On metrics for error correction in network coding. *Information Theory, IEEE Transactions on*, 55(12):5479 –5490, dec. 2009.

[16] D. Silva, F.R. Kschischang, and R. Kötter. A rank-metric approach to error control in random network coding. *Information Theory, IEEE Transactions on*, 54(9):3951–3967, Sept. 2008.

[17] V. Skachek. Recursive code construction for random networks. *Information Theory, IEEE Transactions on*, 56(3):1378 –1382, March 2010.

[18] A.-L. Trautmann, F. Manganiello, M. Braun, and J. Rosenthal. Cyclic orbit codes. *arXiv:1112.1238*, [cs.IT], December 2011.

[19] A.-L. Trautmann, F. Manganiello, and J. Rosenthal. Orbit codes - a new concept in the area of network coding. In *Information Theory Workshop (ITW), 2010 IEEE*, pages 1–4, Dublin, Ireland, August 2010.